readme.gseis.ucla.edu

uclareadme@riseup.net

twitter.com/uclareadme

CREATED FOR
visions of justice and liberation

May 18th, 2018.
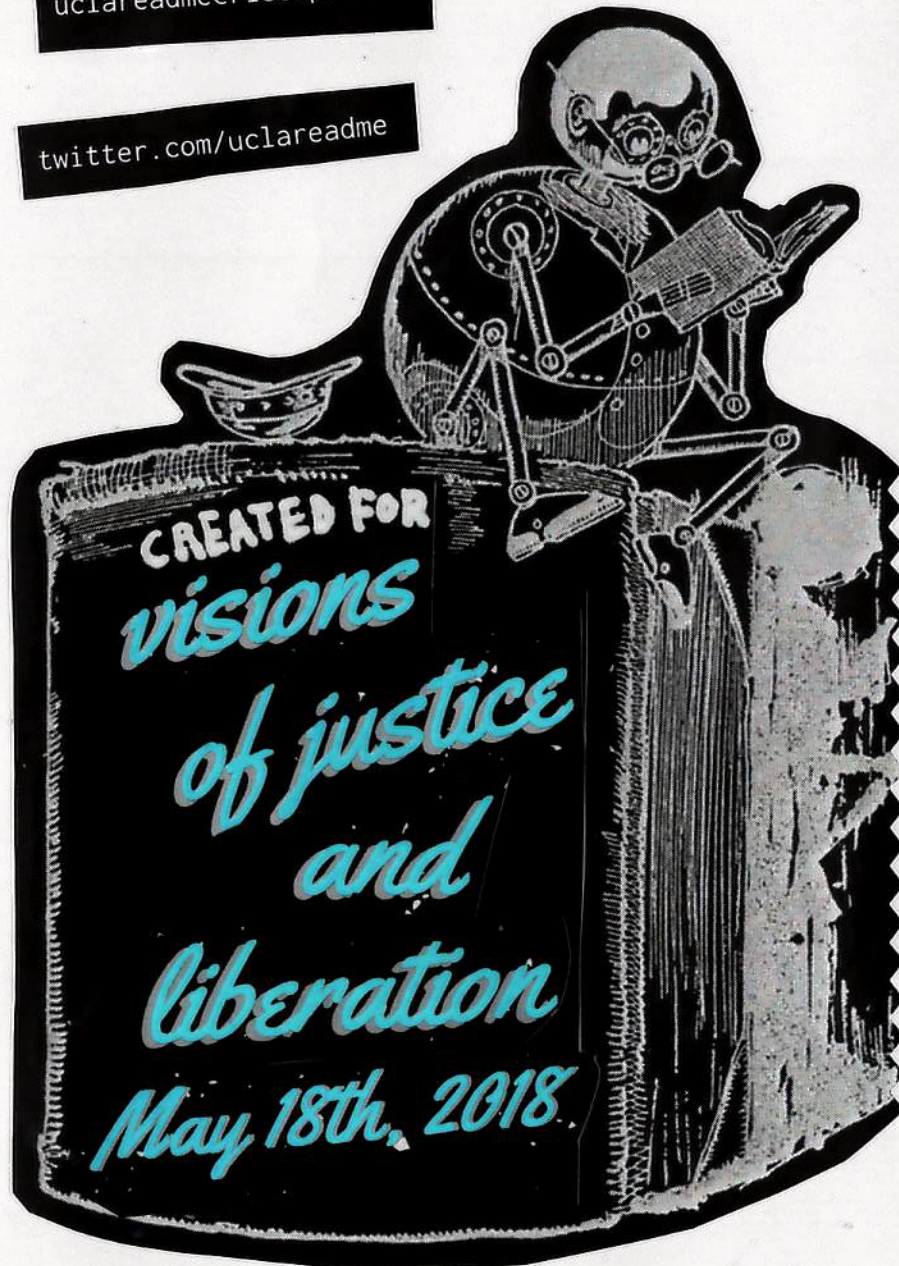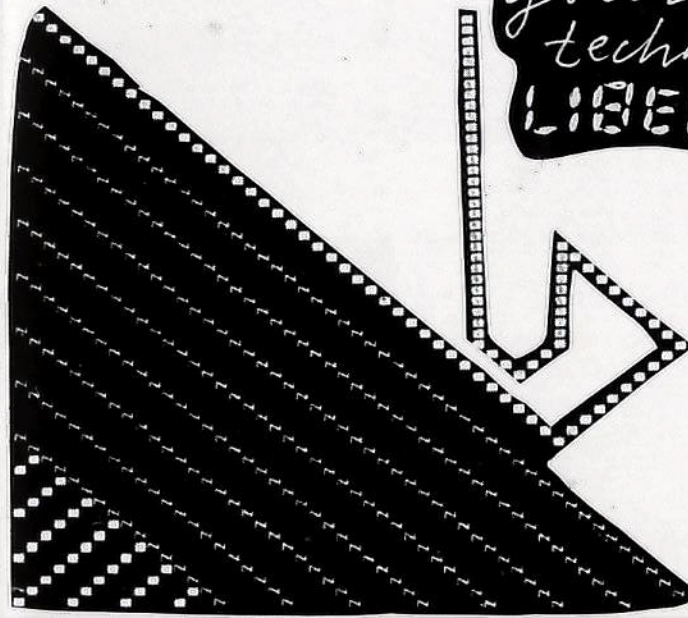
SPECIAL ISSUE!

README

PRESENTS

A BRIEF GUIDE TO
your technological
LIBERATION

```
 |__ |  _| _| _| \|  |  _|
 |__| |__|__|__|__/|_|_|_|___
```

Please Stand by — Jacking In...

TABLE OF CONTENTS

LIBRARY SCHOOL

WE ARE...

UCLA

Information Studies

Students for Digital Rights

README advocates for digital rights including privacy, security, access, and intellectual freedom within libraries, archives, and information work. Initiated by UCLA MLIS students in 2016, README also welcomes IS PhD students and faculty and seeks bridges to other organizations on the UCLA campus and in its libraries.

Teaching Resources

CryptoParty.in <https://www.cryptoparty.in>

EFF: Security Education Companion <https://sec.eff.org>

How To Give A Digital Security Training <https://medium.com/@geminiimatt/how-to-give-a-digital-security-training-4c83af667d40>
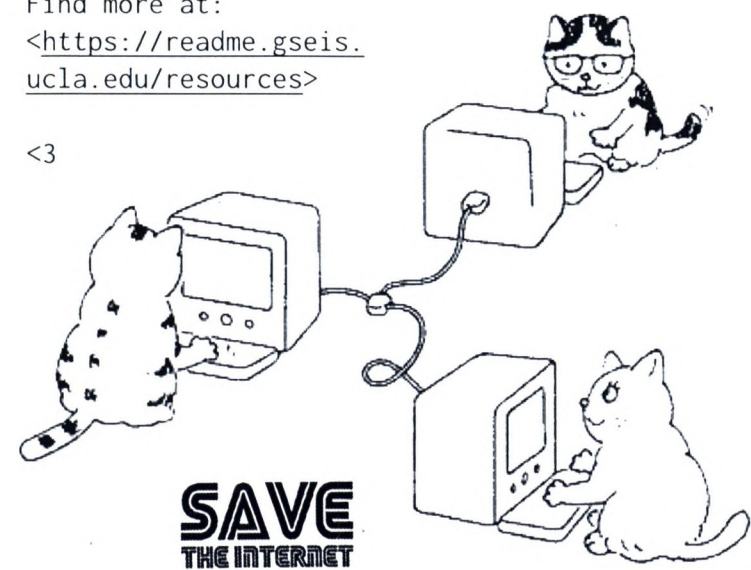
Podcasts

If Then <http://www.slate.com/articles/podcasts/if_then.html>

IRL with Veronica Belmont <https://irlpodcast.org>

Library Bytegeist Episode 6: Talking Privacy with Librarians <https://soundcloud.com/library-bytegeist/6-talking-privacy-with-librarians>

Find more at:
<https://readme.gseis.ucla.edu/resources>

<3

SAVE
THE INTERNET

RESOURCES

The Center for Media Justice
<http://centerformediajustice.org>

Choose Privacy Week <https://chooseprivacyweek.org>

Crypto.la <http://crypto.la>

Electronic Frontier Alliance <https://www.eff.org/electronic-frontier-alliance>

Library Freedom Project <https://libraryfreedomproject.org>

Security in a Box <https://securityinabox.org>

Stop LAPD Spying Coalition <https://stoplapdspying.org>

Tactical Tech <https://tacticaltech.org>

THE CENTER FOR MEDIA JUSTICE

TACTICAL TECHNOLOGY COLLECTIVE

Zines and Guides on Personal Privacy & Security

Chayn: Do It Yourself Online Safety <http://chayn.co/safety>

HACK*BLOSSOM: A DIY Guide to Feminist Cybersecurity <https://hackblossom.org/cybersecurity>
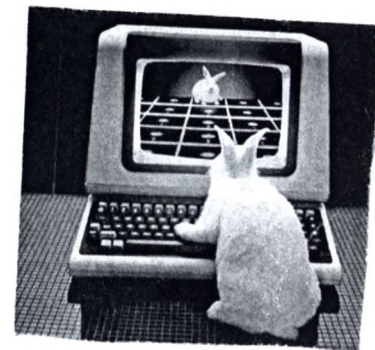
Protect Yourself: a primer on digital and physical resistance <https://www.britt-paris.net/protect-yourself.html>

Tactical Tech: The 8-Day Data Detox Kit <https://datadetox.myshadow.org>

Previous guests include:
Stop LAPD spying
Michelle Forelle, USC PhD
Jon Kyle, @jondashkyle

LAB HOURS

READY LAB HOURS ARE AN UNSTRUCTURED TIME

#READMELabHour

We meet once a week in the IS Lab Room 102 GSE&IS BUILDING

http://readme.gseis.ucla.edu/lab-hours

TOPICS HAVE INCLUDED • DMCA • NET NEUTRALITY • PEER-TO-PEER WEB • INTERNET HEALTH • RIGHT TO REPAIR

No technical knowledge required

Whooooooooops

GOOGLE

climate change is|

climate change is **not real**
climate change is **real**
climate change is **a hoax**
climate change is **fake**
climate change isn't **real**

GOOGLE

islamists are|

islamists are **not our friends**
islamists are **coming**
islamists are **evil**
islamists are **nuts**
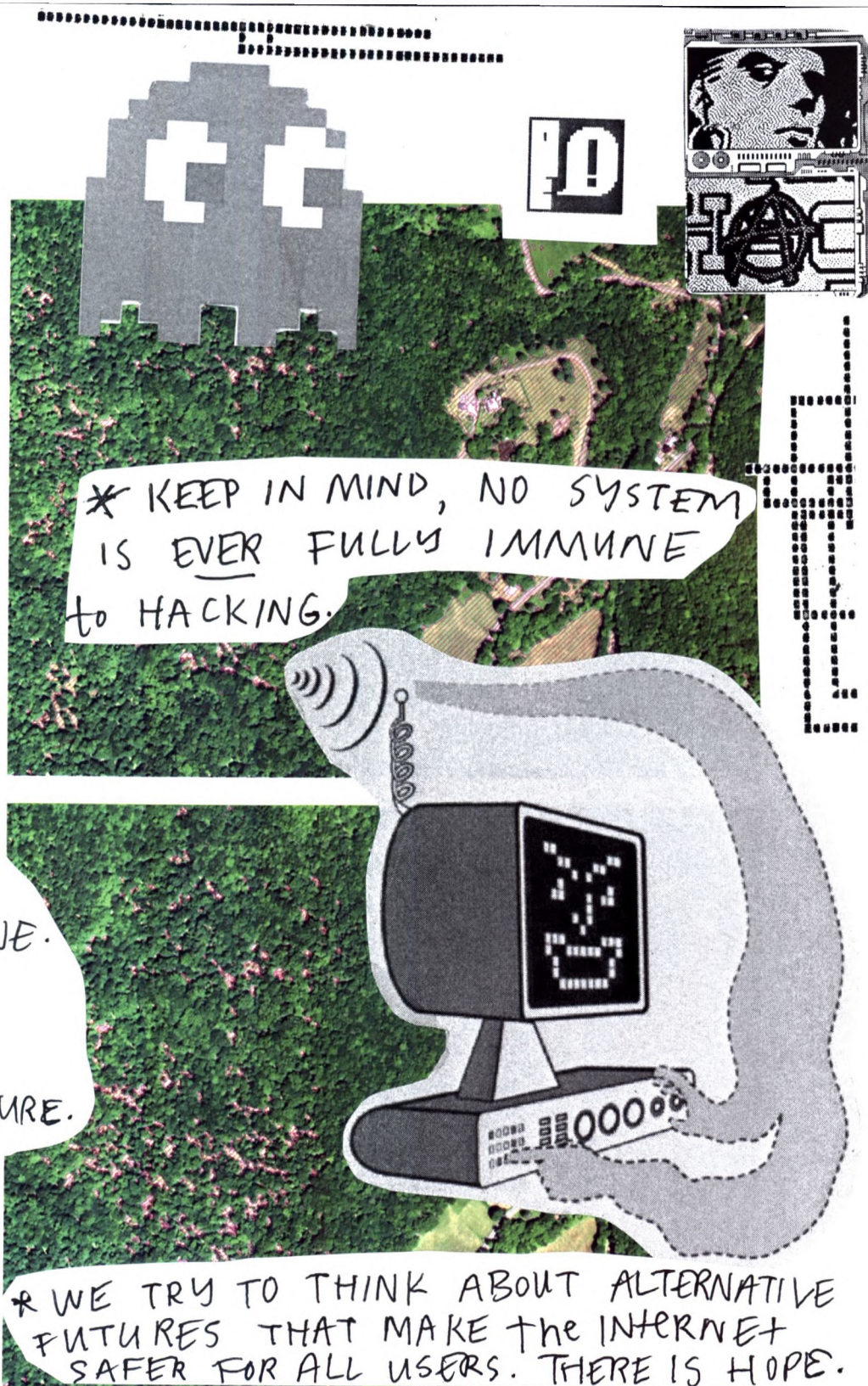islamists are **stupid**
islamists are **terrorists**

How do Big Data algorithms influence the way we access information?

Who makes these algorithms and what cultural biases are embedded within?

How can information professionals level the playing field?

The search engine that doesn't track you!

DuckDuckGo

"Big Data processes codify the past. They do not invent the future. Doing that requires moral imagination, and that's something only humans can provide. We have to explicitly embed better values into our algorithms, creating Big Data models that follow our ethical lead. Sometimes that will mean putting fairness ahead of profit."

from →
by →

WEAPONS OF

MATH DESTRUCTION

HOW BIG DATA INCREASES INEQUALITY

AND THREATENS DEMOCRACY

CATHY O'NEIL

* KEEP IN MIND, NO SYSTEM IS EVER FULLY IMMUNE TO HACKING.

NE.

URE.

* WE TRY TO THINK ABOUT ALTERNATIVE FUTURES THAT MAKE THE INTERNET SAFER FOR ALL USERS. THERE IS HOPE.

IF YOU WANT TO BE A GHOST...

✳ USING TOR AS YOUR WEB BROWSER IS A GOOD WAY TO INSURE A HIGH-LEVEL OF ANONYMITY ONLINE. BUT AVOID USING SITES LIKE FACEBOOK THAT RELY ON YOUR PERSONAL INFORMATION
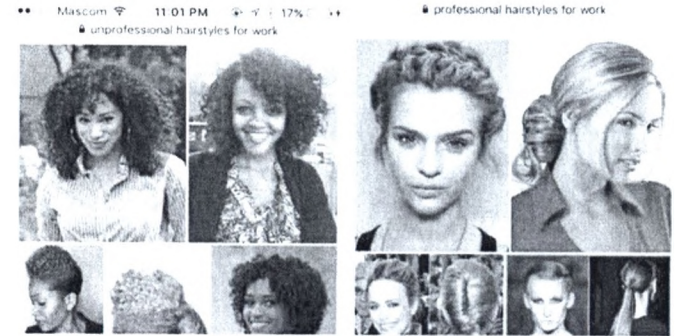
✳ TRY ALTERNATIVE OPERATING SYSTEMS LIKE QUBES OR TAILS. TAILS EXISTS ON A USB FLASH DRIVE and DOESN'T STORE ANY INFORMATION IN BETWEEN SESSIONS. ALL INTERNET ACTIVITY WILL GO THROUGH TOR and YOUR INTERNET CONNECTION WILL BE UNLINKED FROM YOUR MACHIN... QUBES, USING MULTIPLE VIRTUAL machines, KEEPS YOUR ACTIVITY + INFORMATION ISOLATED - THUS MORE SEC...

Rosalia

Follow

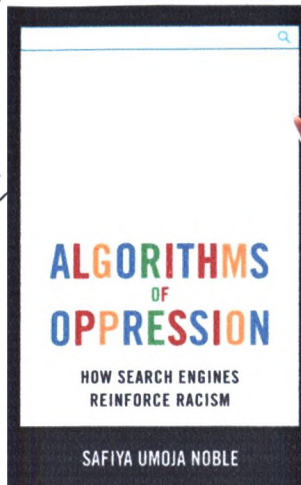I saw a tweet saying "Google unprofessional hairstyles for work". I did. Then I checked the 'professional' ones 🙈 🙈 🙈

Tweet about Google searches on "unprofessional hairstyles for work," which all feature Black women, while "professional hairstyles for work" feature White women. April 7, 2016.

"The implications of such marginalization are profound. The insights about sexist and racist biases...are important because information organizations, from libraries to schools and universities to governmental agencies, are increasingly reliant on being displaced by a variety of web-based "tools" as if there are no political, social, or economic consequences of doing so." — From

Safiya Umoja Noble

ALGORITHMS
OF
OPPRESSION

HOW SEARCH ENGINES REINFORCE RACISM

SAFIYA UMOJA NOBLE

Predictive Policing

"PredPol software, marketed by a private company, relies on a machine-learning algorithm much like the ones used by corporate giants such as Facebook and Amazon for advertising purposes. It's a mathematical model that inputs three variables: where a crime was committed, when it was committed, and what type of crime it was. The model is used to calculate "hot spots" throughout a given metropolitan area —150 square-meter areas where, theoretically, certain types of crimes are more likely to be committed on a given day — which patrol officers use to plan out their daily routes. Studies have already shown that PredPol technology re-enforces racially biased policing patterns and practices, but the technology remains in use by the LAPD and at least 50 other law enforcement agencies around the country, according to a PredPol spokesperson."
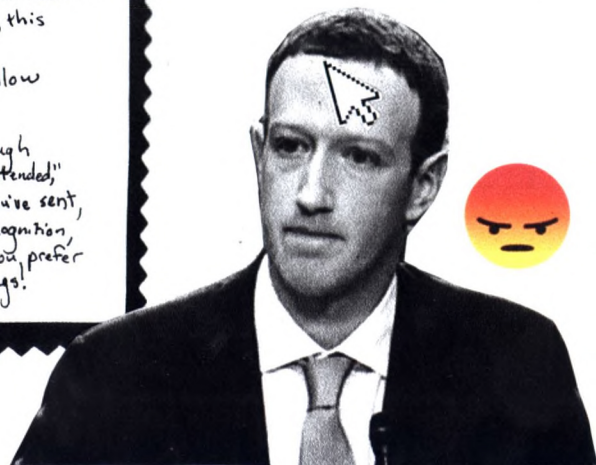
BEFORE THE BULLET HITS THE BODY

Dismantling

Predictive Policing

in Los Angeles

May 8th 2018

Predictive policing refers to a range of policing practices that claim to use pre-existing demographic, environmental, and historic crime data to predict future patterns of crime as well as presuming "where crime will occur," and "who" will commit crime. Predictive policing can be best understood within the broader creep of data-intensive surveillance on the part of law enforcement.

FIND THIS REPORT ↑
@ STOPLAPDSPYING.ORG

FROM "AIDED BY PALANTIR, THE LAPD USES PREDICTIVE POLICING TO MONITOR SPECIFIC PEOPLE AND NEIGHBORHOODS" by Maha Ahmed for THEINTERCEPT.COM

What does Facebook Know about YOU?
If you have an account, there's an easy way to find out:

① Click the down arrow on your account and open settings

② At the bottom, you'll see a link called "download a copy of your Facebook data" Click it!

③ On this page, click "Download Archive" and enter your password

④ You'll be sent an email with your archive. Depending on the size of your file, this should take ~20 min

⑤ A time-sensitive link will allow you to download a .zip file

⑥ You should be able to browse through a list of every event you've ever "attended," video or photo uploaded, messages you've sent, all the images compiled for facial recognition, what advertising topics it thinks you prefer and whole host of other invasive things!

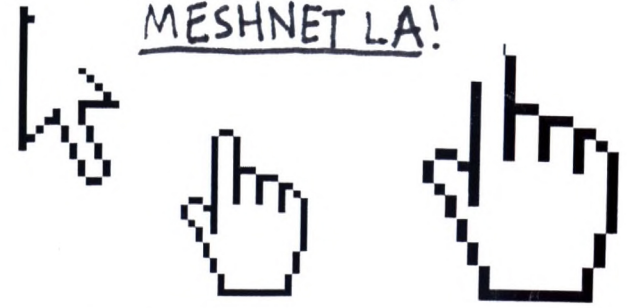FOR ORGANIZING ONLINE, TRY USING ALTERNATIVES TO FACEBOOK LIKE RISEUP.NET

✳ BE WARY OF USING YOUR CELL PHONE and DO WHAT you CANT to ENCRYPT YOUR messages, calls, and BROWSING ACTIVITY.

HELP BUILD THE DECENTRALIZED NET

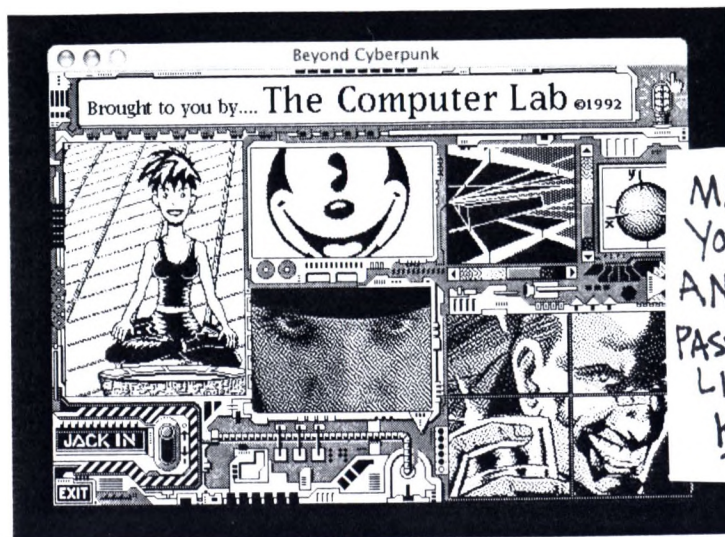SEEK OUT AND SUPPORT YOUR LOCAL MESH NET-WORK! CHECK OUT MESHNET LA!

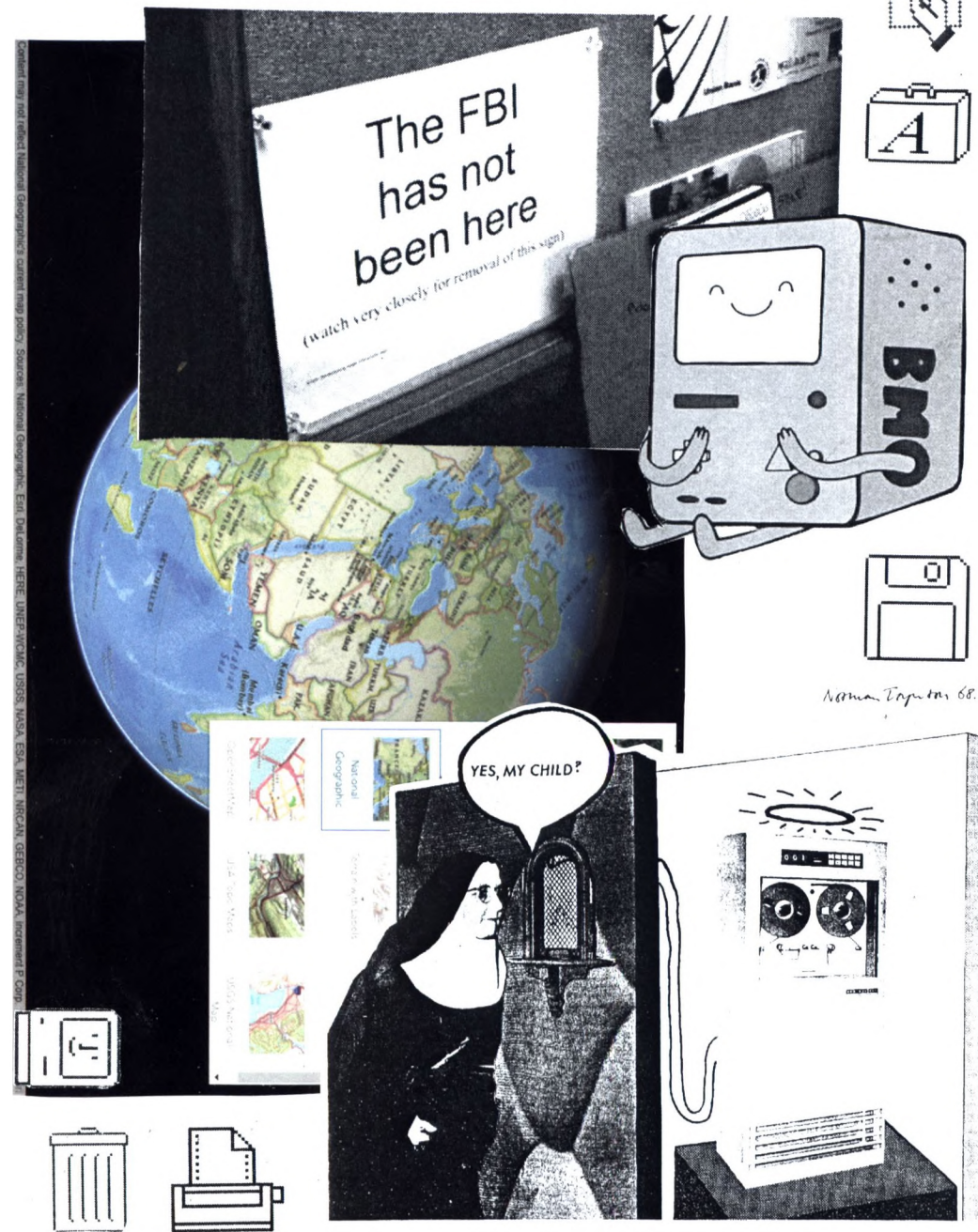IF YOU KNOW SOME BASICS, BUT FEEL LIKE YOU WANT TO DO MORE...

* IMPROVE YOUR OVERALL SECURITY WITH A VPN OR VIRTUAL PRIVATE NETWORK - WHICH TUNNELS YOUR internet activity through a PRIVATE NETWORK and tell WEBSITES THAT YOUR LOCATED SOMEWHERE ELSE.

* USE TWO-FACTOR AUTHENTICATION WHENEVER POSSIBLE!

Beyond Cyberpunk
Brought to you by.... The Computer Lab ©1992

JACK IN
EXIT

MAKE SURE YOU'RE USING AN ENCRYPTED PASSWORD MANAGER LIKE: KEEPASSXC

QUESTIONS TO ASK WHEN DEALING WITH EVIL COMPUTERS

The FBI has not been here
(watch very closely for removal of this sign)

BMO

YES, MY CHILD?

Norman Trapisso 68.

IF YOU'RE JUST STARTING OUT...

*be cautious of public WI-FI – it's not as secure as you may think.

* CHECK your privacy settings and update them to be as secure as possible.

* COVER the built-in camera on your computer.

* don't login to any WEBSITE with your social media accounts.

LIBRARIANS AGAINST DRM

BIG DATA? NO THANKS

* Consider downloading BROWSER extensions like PRIVACY BADGER or HTTPS everywhere.

CHECK OUT THE ELECTRONIC FRONTIER FOUNDATION @ SSD.EFF.ORG

ARE YOU USING?	TRY USING...
• CHROME	• FIREFOX
• TEXT MESSAGING like iMESSAGE etc.	• SIGNAL
• GOOGLE	• DUCKDUCKGO
• THE SAME PASSWORD for EVERYTHING with YOUR BIRTHDAY in it	• A PASSWORD MANAGER and RANDOMLY GENERATED, COMPLEX PASSWORDS
• GMAIL	• PROTONMAIL or FASTMAIL *not-encrypted

EFA